Derwent Data Available on Delphio

Delphion

ABOUT DELPHION | **PRODUCTS** | **NEWS & EVENTS** | **IP RESOURCES** | IP Si

Search   Login   Register   Order Form   Shopping Cart   Premium Features

Inquire Regarding Licensing

US5949876:Systems and methods for secure transaction management and electronic rights protection

No Image | Expand Details | View Cart | View INPADOC only | Derwent Record...

Add to cart: More choices...

|	
Inventor(s):	**Ginter; Karl L.** , Beltsville, MD **Shear; Victor H.** , Bethesda, MD **Spahn; Francis J.** , El Cerrito, CA **Van Wie; David M.** , Sunnyvale, CA
Applicant(s):	**InterTrust Technologies Corporation**, Sunnyvale, CA News, Profiles, Stocks and More about this company
Issued/Filed Dates:	Sept. 7, 1999 / Jan. 8, 1997
Application Number:	US1997000778256
IPC Class:	H04L 9/32;
Class:	Current: 705/080; 705/001; 705/039; 705/054; Original: 380/004; 380/024; 705/039;
Field of Search:	395/237,241 380/4,16,49,24 705/039
Legal Status:	Show legal status actions

Abstract:

The present invention provides systems and methods for secure transaction management and electronic rights protection. Electronic appliances such as computers equipped in accordance with the present invention help to ensure that information is accessed and used only in authorized ways, and maintain the integrity, availability, and/or confidentiality of the information. Such electronic appliances provide a distributed virtual distribution environment (VDE) that may enforce a secure chain of handling and control, for example, to control and/or meter or otherwise monitor use of electronically stored or disseminated information. Such a virtual distribution environment may be used to protect rights of various participants in electronic commerce and other electronic or electronic-facilitated transactions. Distributed and other operating systems, environments and architectures, such as, for example, those using tamper-resistant hardware-based processors, may establish security at each node. These techniques may be used to support an all-electronic information distribution, for example, utilizing the "electronic highway."

Patent Plaques
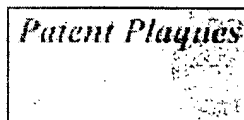
Attorney, Agent, or	**Nixon & Vanderhye P.C.;**

Firm:	■
Primary/Assistant Examiners:	**Barron, Jr.; Gilberto;** ■

Related Applications:

Application Number	ApplDate	Patent	Issued	Title
US1995000388107	1995-02-13			

Family: Show known family members
■

U.S. References: | Show the 5 patents that reference this one

Patent	Issued	Inventor(s)	Applicant(s)	Title
US4309569	1 /1982	Merkle	The Board of Trustees of the Leland Stanford Junior University	Method of providing digital signatures
US4337483	6 /1982	Guillou	Etablissement Public de Diffusion dit "Telediffusion de France"	Text video-transmission system provided with means for controlling access to the information
US4465901	8 /1984	Best		Crypto microprocessor that executes enciphered programs
US4558176	12 /1985	Arnold et al.		Computer systems to inhibit unauthorized copying, unauthorized usage, and automated cracking of protected software
US4672572	6 /1987	Alsberg	Gould Inc.	Protector system for computer access and use
US4713753	12 /1987	Boebert et al.	Honeywell Inc.	Secure data processing system architecture with format control
US4757534	7 /1988	Matyas et al.	International Business Machines Corporation	Code protection using cryptography
US4796181	1 /1989	Wiedemer		Billing system for computer software
US4799156	1 /1989	Shavit et al.	Strategic Processing Corporation	Interactive market management system
US4807288	2 /1989	Ugon et al.	C.I.I. Honeywell Bull	Microprocessor intended particularly for executing the calculation algorithms of a public code encoding system
US4817140	3 /1989	Chandra et al.	International Business Machines Corp.	Software protection system using a single-key cryptosystem, a hardware-based authorization system and a secure coprocessor
US4823264	4 /1989	Deming		Electronic funds transfer system
US4858121	8 /1989	Barber et al.	Medical Payment Systems, Incorporated	Medical payment system
US4864494	9 /1989	Kobus	Computerized Data Ssytems for Mfg.,	Software usage authorization system with key for decrypting/re-encrypting/re-transmitting moving target security

			Inc.	moving target security codes from protected software
US4868877	9 /1989	Fischer		Public key/signature cryptosystem with enhanced digital signature certification
US4903296	2 /1990	Chandra et al.	International Business Machines Corporation	Implementing a shared higher level of privilege on personal computers for copy protection of software
US4930073	5 /1990	Cina, Jr.	International Business Machines Corporation	Method to prevent use of incorrect program version in a computer system
US4999806	3 /1991	Chernow et al.		Software distribution system
US5005200	4 /1991	Fischer		Public key/signature cryptosystem with enhanced digital signature certification
US5047928	9 /1991	Wiedemer		Billing system for computer software
US5091966	2 /1992	Bloomberg et al.	Xerox Corporation	Adaptive scaling for decoding spatially periodic self-clocking glyph shape codes
US5103476	4 /1992	Waite et al.		Secure system for activating personal computer software at remote locations
US5111390	5 /1992	Ketcham	Unisys Corporation	Software security system for maintaining integrity of compiled object code by restricting users ability to define compilers
US5128525	7 /1992	Stearns et al.	Xerox Corporation	Convolution filtering for decoding self-clocking glyph shape codes
US5136643	8 /1992	Fischer		Public/key date-time notary facility
US5136646	8 /1992	Haber et al.	Bell Communications Research, Inc.	Digital document time-stamping with catenate certificate
US5136647	8 /1992	Haber et al.	Bell Communications Research, Inc.	Method for secure time-stamping of digital documents
US5146575	9 /1992	Nolan, Jr.	International Business Machines Corp.	Implementing privilege on microprocessor systems for use in software asset protection
US5155680	10 /1992	Wiedemer	Signal Security Technologies	Billing system for computing software
US5168147	12 /1992	Bloomberg	Xerox Corporation	Binary image processing for decoding self-clocking glyph shape codes
US5185717	2 /1993	Mori		Tamper resistant module having logical elements arranged in multiple layers on the outer surface of a substrate to protect stored information
				Relational database

US5201046	4 /1993	Goldberg et al.	Xidak, Inc.	management system and method for storing, retrieving and modifying directed graph data structures
US5201047	4 /1993	Maki et al.	International Business Machines Corporation	Attribute-based classification and retrieval system
US5208748	5 /1993	Flores et al.	Action Technologies, Inc.	Method and apparatus for structuring and managing human communications by explicitly defining the types of communications permitted between participants
US5214702	5 /1993	Fischer		Public key/signature cryptosystem with enhanced digital signature certification
US5216603	6 /1993	Flores et al.	Action Technologies, Inc.	Method and apparatus for structuring and managing human communications by explicitly defining the types of communications permitted between participants
US5221833	6 /1993	Hecht	Xerox Corporation	Methods and means for reducing bit error rates in reading self-clocking glyph codes
US5222134	6 /1993	Waite et al.	Tau Systems Corporation	Secure system for activating personal computer software at remote locations
US5224160	6 /1993	Paulini et al.	Siemens Nixdorf Informationssysteme AG	Process for securing and for checking the integrity of the secured programs
US5224163	6 /1993	Gasser et al.	Digital Equipment Corporation	Method for delegating authorization from one entity to another through the use of session encryption keys
US5235642	8 /1993	Wobber et al.	Digital Equipment Corporation	Access control subsystem and method for distributed computer system using locally cached authentication credentials
US5245165	9 /1993	Zhang	Xerox Corporation	Self-clocking glyph code for encoding dual bit digital values robustly
US5247575	9 /1993	Sprague et al.		Information distribution system
US5260999	11 /1993	Wyman	Digital Equipment Corporation	Filters in license management system
US5265164	11 /1993	Matyas et al.	International Business Machines Corporation	Cryptographic facility environment backup/restore and replication in a public key cryptosystem
US5276735	1 /1994	Boebert et al.	Secure Computing Corporation	Data enclave and trusted path system
US5280479	1 /1994	Mary	Matra Communication	Device for insertion of digital packets in a

			Communication	transmission channel
US5285494	2 /1994	Sprecher et al.	PacTel Corporation	Network management system
US5301231	4 /1994	Abraham et al.	International Business Machines Corporation	User defined function facility
US5319705	6 /1994	Halter et al.	International Business Machines Corporation	Method and system for multimedia access control enablement
US5337360	8 /1994	Fischer		Method and apparatus for creating, supporting, and using travelling programs
US5341429	8 /1994	Stringer et al.	TestDrive Corporation	Transformation of ephemeral material
US5343527	8 /1994	Moore	International Business Machines Corporation	Hybrid encryption method and system for protecting reusable software components
US5347579	9 /1994	Blandford		Personal computer diary
US5351293	9 /1994	Michener et al.	Wave Systems Corp.	System method and apparatus for authenticating an encrypted signal
US5355474	10 /1994	Thuraisngham et al.		System for multilevel secure database management using a knowledge base with release-based and other security constraints for query, response and update modification
US5365587	11 /1994	Campbell et al.	International Business Machines Corporation	Self modifying access code for altering capabilities
US5373561	12 /1994	Haber et al.	Bell Communications Research, Inc.	Method of extending the validity of a cryptographic certificate
US5390247	2 /1995	Fischer		Method and apparatus for creating, supporting, and using travelling programs
US5390330	2 /1995	Talati		Control system and method for direct execution of software application information models without code generation
US5392220	2 /1995	van den Hamer et al.	U.S. Philips Corporation	Method and system for organizing data
US5392390	2 /1995	Crozier	IntelliLink Corp.	Method for mapping, translating, and dynamically reconciling data between disparate computer platforms
US5394469	2 /1995	Nagel et al.	Infosafe Systems, Inc.	Method and apparatus for retrieving secure information from mass storage media
US5412717	5 /1995	Fischer		Computer system security method and apparatus having program authorization information data structures
			Compaq Computer	Method and apparatus for

US5421006	5 /1995	Jablon	Compaq Computer Corp.	assessing integrity of computer system software
US5422953	6 /1995	Fischer		Personal date/time notary device
US5428606	6 /1995	Moskowitz		Digital information commodities exchange
US5442645	8 /1995	Ugon	Bull CP8	Method for checking the integrity of a program or data, and apparatus for implementing this method
US5444779	8 /1995	Daniele	Xerox Corporation	Electronic copyright royalty accounting system using glyphs
US5449895	9 /1995	Hecht et al.	Xerox Corporation	Explicit synchronization for self-clocking glyph codes
US5449896	9 /1995	Hecht et al.	Xerox Corporation	Random access techniques for use with self-clocking glyph codes
US5450493	9 /1995	Maher	AT&T Corp.	Secure communication method and apparatus
US5453605	9 /1995	Hecht et al.	Xerox Corporation	Global addressability for self-clocking glyph codes
US5455861	10 /1995	Faucher et al.	AT&T Corp.	Secure telecommunications
US5455953	10 /1995	Russell	Wang Laboratories, Inc.	Authorization system for obtaining in single step both identification and access rights of client to server directly from encrypted authorization ticket
US5457746	10 /1995	Dolphin	Spyrus, Inc.	System and method for access control for portable data storage media
US5463565	10 /1995	Cookson et al.	Time Warner Entertainment Co., L.P.	Data block format for software carrier and player therefor
US5473687	12 /1995	Lipscomb et al.	Infosafe Systems, Inc.	Method for retrieving secure information from a database
US5473692	12 /1995	Davis	Intel Corporation	Roving software license for a hardware agent
US5479509	12 /1995	Ugon	Bull CP8	Method for signature of an information processing file, and apparatus for implementing it
US5485622	1 /1996	Yamaki	Kabushiki Kaisha Toshiba	Password processing system for computer
US5491800	2 /1996	Goldsmith et al.	Taligent, Inc.	Object-oriented remote procedure call networking system
US5497479	3 /1996	Hornbuckle	SofTel, Inc.	Method and apparatus for remotely controlling and monitoring the use of computer software
US5497491	3 /1996	Mitchell et al.	International Business Machines	System and method for importing and exporting data between an object oriented computing environment and an

			Corporation	environment and an external computing environment
US5499298	3 /1996	Narasimhalu et al.	National University of Singapore	Controlled dissemination of digital information
US5504757	4 /1996	Cook et al.	International Business Machines Corporation	Method for selecting transmission speeds for transmitting data packets over a serial bus
US5504818	4 /1996	Okano		Information processing system using error-correcting codes and cryptography
US5504837	4 /1996	Griffeth et al.	Bell Communications Research, Inc.	Method for resolving conflicts among distributed entities through the generation of counter proposals by transversing a goal hierarchy with acceptable, unacceptable, and indeterminate nodes
US5508913	4 /1996	Yamamoto et al.	Fujitsu Limited	Electronic automatic offer matching system for freezer exchange transactions among banks
US5509070	4 /1996	Schull	SoftLock Services Inc.	Method for encouraging purchase of executable and non-executable software
US5513261	4 /1996	Maher	AT&T Corp.	Key management scheme for use with electronic cards
US5530235	6 /1996	Stefik et al.	Xerox Corporation	Interactive contents revealing storage device
US5530752	6 /1996	Rubin	Convex Computer Corporation	Systems and methods for protecting software from unlicensed copying and use
US5533123	7 /1996	Force et al.	National Semiconductor Corporation	Programmable distributed personal security
US5534975	7 /1996	Stefik et al.	Xerox Corporation	Document processing system utilizing document service cards to provide document processing services
US5537526	7 /1996	Anderson et al.	Taugent, Inc.	Method and apparatus for processing a display document utilizing a system level document framework
US5539735	7 /1996	Moskowitz		Digital information commodities exchange
US5539828	7 /1996	Davis	Intel Corporation	Apparatus and method for providing secured communications
US5550971	8 /1996	Brunner et al.	U S West Technologies, Inc.	Method and system for generating a user interface adaptable to various database management systems
US5553282	9 /1996	Parrish et al.	Taligent, Inc.	Software project history database and method of

				operation
US5563946	10 /1996	Cooper et al.	International Business Machines Corporation	Method and apparatus for enabling trial period use of software products: method and apparatus for passing encrypted files between data processing systems
US5568552	10 /1996	Davis	Intel Corporation	Method for providing a roving software license from one node to another node
US5572673	11 /1996	Shurts	Sybase, Inc.	Secure multi-level system for executing stored procedures
US5592549	1 /1997	Nagel et al.	Infosafe Systems, Inc.	Method and apparatus for retrieving selected information from a secure information source
US5606609	2 /1997	Houser et al.	Scientific-Atlanta	Electronic document verification system and method
US5613004	3 /1997	Cooperman et al.	The Dice Company	Steganographic method and device
US5621797	4 /1997	Rosen	Citibank, N.A.	Electronic ticket presentation and transfer method
US5629980	5 /1997	Stefik et al.	Xerox Corporation	System for controlling the distribution and use of digital works
US5633932	5 /1997	Davis et al.	Intel Corporation	Apparatus and method for preventing disclosure through user-authentication at a printing node
US5634012	5 /1997	Stefik et al.	Xerox Corporation	System for controlling the distribution and use of digital works having a fee reporting mechanism
US5636292	6 /1997	Rhoads	Digimarc Corporation	Steganography methods employing embedded calibration data
US5638443	6 /1997	Stefik et al.	Xerox Corporation	System for controlling the distribution and use of composite digital works
US5638504	6 /1997	Scott et al.	Object Technology Licensing Corp.	System and method of processing documents with document proxies
US5640546	6 /1997	Gopinath et al.	Network Programs, Inc.	Composition of systems of objects by interlocking coordination, projection, and distribution
US5655077	8 /1997	Jones et al.	Microsoft Corporation	Method and system for authenticating access to heterogeneous computing services
US5687236	11 /1997	Moskowitz et al.	The Dice Company	Steganographic method and device
US5689587	11 /1997	Bender et al.	Massachusetts Institute of Technology	Method and apparatus for data hiding in images
US5692180	11 /1997	Lee	International Business Machines	Object-oriented cell directory database for a

US5692180	11/1997	Lee	Business Machines Corporation	distributed computing environment
US5710834	1/1998	Rhoads	Digimarc Corporation	Method and apparatus responsive to a code signal conveyed through a graphic image
US5740549	4/1998	Reilly et al.	PointCast, Inc.	Information and advertising distribution system and method
US5745604	4/1998	Rhoads	Digimarc Corporation	Identification/authentication system using robust, distributed coding
US5748763	5/1998	Rhoads	Digimarc Corporation	Image steganography system featuring perceptually adaptive and globally scalable signal embedding
US5748783	5/1998	Rhoads	Digimarc Corporation	Method and apparatus for robust information coding
US5748960	5/1998	Fischer		Method and apparatus for validating travelling object-oriented programs with digital signatures
US5754849	5/1998	Dyer et al.	Wayfarer Communications, Inc.	Self-describing object providing dynamic manipulation of heterogeneous data values and semantic identity between memory and transmission representations
US5757914	5/1998	McManis	Sun Microsystems, Inc.	System and method for protecting use of dynamically linked executable modules
US5758152	5/1998	LeTourneau	Prime Arithmetics, Inc.	Method and apparatus for the generation and manipulation of data structures
US5765152	1/1998	Erickson	Trustees of Dartmouth College	System and method for managing copyrighted electronic media
US5768426	6/1998	Rhoads	Digimarc Corporation	Graphics processing system employing embedded code signals

CLAIMS:
[Hide claims]:

We claim:
1. A method for negotiating electronic contracts, comprising:

- receiving a first control set from a remote site;
- providing a second control set;
- performing, within a protected processing environment, an electronic negotiation between said first control set and said second control set, including providing interaction between said first and second control sets; and
- producing a negotiated control set resulting from said interaction between said first and second control sets.

2. A system for supporting electronic commerce including:

- means for creating a first secure control set at a first location;
- means for creating a second secure control set at a second location;
- means for securely communicating said first secure control set from said first location to said second location; and
- means at said second location for securely integrating said first and second control sets to produce at least a third control set comprising plural elements together comprising an electronic value chain extended agreement.

3. A system for supporting electronic commerce including:

- means for creating a first secure control set at a first location;
- means for creating a second secure control set at a second location;
- means for securely communicating said first secure control set from said first location to said second location; and
- negotiation means at said second location for negotiating an electronic contract through secure execution of at least a portion of said first and second secure control sets.

4. A system as in claim 3 further including means for controlling use by a user of protected information content based on at least a portion of said first and/or second control sets.

5. A system as in claim 3 further including means for charging for at least a part of said content use.

6. A system for negotiating electronic contracts, comprising:

- a storage arrangement that stores a first control set received from a remote site, and stores a second control set;
- a protected processing environment, coupled to said storage arrangement, that:
- (a) performs an electronic negotiation between said first control set and said second control set,
- (b) provides interaction between said first and second control sets, and
- (c) produces a negotiated control set resulting from said interaction between said first and second control sets.

7. A system as in claim 6 further including means for electronically enforcing said negotiated control set.

8. A system as in claim 6 further including means for generating an electronic contract based on said negotiated control set.

9. A method for supporting electronic commerce including:

- creating a first secure control set at a first location;
- creating a second secure control set at a second location;
- securely communicating said first secure control set from said first location to said second location; and
- electronically negotiating, at said second location, an electronic contract, including the step of securely executing at least a portion of said first and second secure control sets.

10. A method as in claim 1 in which said steps of receiving, providing, performing and producing occur within a Virtual Distribution Environment.

11. A system as in claim 2 in which said first location and said second location are contained within a Virtual Distribution Environment.

12. A system as in claim 3 in which said first location and said

second location are contained within a Virtual Distribution Environment.

13. A system as in claim 6 in which said protected processing environment is contained within a Virtual Distribution Environment.

14. A method as in claim 9 in which said first location and said second location are contained within a Virtual Distribution Environment.

15. A method as in claim 1 in which said first control set is received from a first remote site;

- said second control set is received from a second remote site; and
- said performing step is produced at a third site which is different from the first remote site and the second remote site.

16. A system as in claim 6 in which said second control set is received from a second remote site; and

- said protected processing environment is located at a third site which is different from said remote site and said second remote site.

17. A method as in claim 1 in which:

- said first control set is generated by or for a first party distributor of protected information content;
- said second control set is generated by or for a second party which desires to use said protected information content;
- said electronic negotiation concerns the terms under which said second party will obtain the right to use said protected information content; and
- said negotiated control set includes terms under which said second party receives the right to use said protected information content.

18. A system as in claim 2 in which:

- said first secure control set includes controls generated at least in part by or for a first party distributor of protected information content;
- said second secure control set includes controls generated at least in part by or for a second party which desires to use said protected information content; and
- said third control set includes controls which govern terms under which said second party receives the right to use said protected information content.

19. A system as in claim 3 in which:

- said first secure control set includes controls generated at least in part by or for a first party distributor of protected information content;
- said second secure control set includes controls generated at least in part by or for a second party which desires to use said protected information content; and
- said electronic contract includes controls which govern terms under which said second party receives the right to use said protected information content.

20. A system as in claim 6 in which:

- said first control set includes controls generated at least in part by or for a first party distributor of protected information content;
- said second control set includes controls generated at least in part by or for a second party which desires to use said protected information content; and
- said negotiated control set includes controls which govern terms under which said second party receives the right to use said protected information content.

21. A method as in claim 9 in which

- said first secure control set includes controls generated at least in part by or for a first party distributor of protected information content;
- said second secure control set includes controls generated at least in part by or for a second party which desires to use said protected information content; and
- said electronic contract includes controls which govern terms under which said second party receives the right to use said protected information content.

22. A method as in claim 1 in which said first control set includes terms which are desired but not required.

23. A method as in claim 1 in which said first control set includes required terms.

24. A method as in claim 2 in which said first control set includes required terms.

25. A method as in claim 1 in which said second control set includes required terms.

26. A method as in claim 1 in which said second control set includes terms which are desired but not required.

27. A method as in claim 26 in which said second control set includes required terms.

28. A system as in claim 2 in which said first secure control set includes terms which are desired but not required.

29. A system as in claim 2 in which said first secure control set includes required terms.

30. A system as in claim 28 in which said first secure control set includes required terms.

31. A system as in claim 2 in which said second secure control set includes terms which are desired but not required.

32. A system as in claim 2 in which said second secure control set includes required terms.

33. A system as in claim 31 in which said second secure control set includes required terms.

34. A system as in claim 3 in which said first secure control set includes terms which are desired but not required.

35. A system as in claim 3 in which said first secure control set includes required terms.

36. A system as in claim 34 in which said first secure control set includes required terms.

37. A system as in claim 3 in which said second secure control set includes terms which are desired but not required.

38. A system as in claim 3 in which said second secure control set includes required terms.

39. A system as in claim 38 in which said second secure control set includes required terms.

40. A system as in claim 6 in which said first control set includes terms which are desired but not required.

41. A system as in claim 6 in which said first control set includes required terms.

42. A system as in claim 40 in which said first control set includes required terms.

43. A system as in claim 6 in which said second control set includes terms which are desired but not required.

44. A system as in claim 6 in which said second control set includes required terms.

45. A system as in claim 43 in which said second control set includes required terms.

46. A method as in claim 9 in which said first secure control set includes terms which are desired but not required.

47. A method as in claim 9 in which said first secure control set includes required terms.

48. A method as in 46 in which said first secure control set includes required terms.

49. A method as in 9 in which said second secure control set includes terms which are desired but not required.

50. A method as in claim 9 in which said second secure control set includes required terms.

51. A method as in claim 49 in which said second secure control set includes required terms.

52. A method as in claim 1 in which said first control set is contained in a first PERC.

53. A method as in claim 52 in which said second control set is contained in a second PERC.

54. A method as in claim 1 in which said negotiated control set is contained in a PERC.

55. A method as in claim 1 in which said electronic negotiation is undertaken pursuant to rules contained in a third control set.

56. A method as in claim 2 in which said third control set is contained in a PERC.

57. A system as in claim 2 in which said first secure control set is contained in a first PERC.

58. A system as in claim 57 in which said second secure control set is contained in a second PERC.

59. A system as in claim 58 in which said third control set is contained in a third PERC.

60. A system as in claim 2 in which said means for securely integrating said first and second control sets includes a fourth control set.

61. A system as in claim 60 in which said fourth control set includes controls which govern said secure integration.

62. A system as in claim 60 in which said fourth control set is contained in a PERC.

63. A system as in claim 3 in which said first secure control set is contained in a PERC.

64. A system as in claim 3 in which said second secure control set is contained in a PERC.

65. A system as in claim 64 in which said negotiation means includes a third secure control set.

66. A system as in claim 65 in which said third secure control set is contained in a PERC.

67. A system as in claim 66 in which said third secure control set includes controls which govern said negotiating of said electronic contract.

68. A system as in claim 66 in which said electronic contract consists of a fourth secure control set.

69. A system as in claim 68 in which said fourth secure control set is contained in a PERC.

70. A system as in claim 6 in which said first control set is contained in a PERC.

71. A system as in claim 70 in which said second control set is contained in a PERC.

72. A system as in claim 71 in which said protected processing environment contains a third control set.

73. A system as in claim 72 in which said third control set is contained in a PERC.

74. A system as in claim 72 in which said third control set includes controls which govern said electronic negotiation.

75. A system as in claim 70 in which said negotiated control set is contained in a PERC.

76. A method as in claim 9 in which said first secure control set is contained in a PERC.

77. A method as in claim 9 in which said second secure control set is contained in a PERC.

78. A method as in claim 9 in which said second location contains a third secure control set.

79. A method as in claim 78 in which said third secure control set is contained in a PERC.

80. A method as in claim 78 in which said third secure control set contains controls which govern, at least in part, said step of electronically negotiating an electronic contract.

81. A method as in claim 78 in which said electronic contract consists of a fourth secure control set.

82. A method as in claim 81 in which said fourth secure control set is contained in a PERC.

83. A method as in claim 1 in which said first control set is made up of controls from at least a first and a second alternate groups of controls.

84. A method as in claim 83 in which said first alternate group of controls includes controls which are shared with said second alternate group of controls and controls which are not shared with said second alternate group of controls.

85. A method as in claim 84 in which said second control set is made up of controls from at least a third and a fourth alternate group of controls.

86. A method as in claim 85 in which said third alternate group of controls includes controls which are shared with said fourth alternate group of controls and controls which are not shared with said fourth alternate group of controls.

87. A method as in claim 83 in which said interaction between said first and second control sets includes a step wherein at least one of the alternate groups of controls from said first control set is selected.

88. A method as in claim 85 in which said interaction between said first and second control sets includes a step wherein at least one of the alternate groups of controls from said second control set is selected.

89. A system as in claim 2 in which said first secure control set is made up of controls from at least two alternate groups of controls.

90. A system as in claim 89 in which said at least two alternate groups of controls include controls which are uniquely in one of said groups, and shared controls which are present in more than one of said groups.

91. A system as in claim 2 in which said second secure control set is made up of controls from at least two alternate groups of controls.

92. A system as in claim 91 in which said at least two alternate groups of controls making up said second control set include controls which are uniquely in one of said groups, and shared controls which are present in more than one of said groups.

93. A system as in claim 89 in which said means at said second location for securely integrating said first and second control sets includes means for selecting at least one of the alternate groups of controls from said first secure control set.

94. A system as in claim 91 in which said means at said second location for securely integrating said first and second control sets includes means for selecting at least one of the alternate groups of controls from said second secure control set.

95. A system as in claim 3 in which said first secure control set is made up of controls from at least two alternate groups of controls.

96. A system as in claim 95 in which said at least two alternate groups of controls include controls which are uniquely in one of said groups, and shared controls which are present in more than one of said groups.

97. A system as in claim 3 in which said second secure control set is made up of controls from at least two alternate groups of controls.

98. A system as in claim 97 in which said at least two alternate

groups of controls making up said second secure control set include controls which are uniquely in one of said groups, and shared controls which are present in more than one of said groups.

99. A system as in claim 95 in which said negotiation means includes means for selecting at least one of the alternate groups of controls from said first secure control set.

100. A system as in claim 97 in which said negotiation means includes means for selecting at least one of the alternate groups of controls from said second secure control set.

101. A system as in claim 6 in which said first control set is made up of controls from at least two alternate groups of controls.

102. A system as in claim 101 in which said at least two alternate groups of controls include controls which are uniquely in one of said groups, and shared controls which are present in more than one of said groups.

103. A system as in claim 6 in which said second control set is made up of controls from at least two alternate groups of controls.

104. A system as in claim 103 in which said at least two alternate groups of controls making up said second control set include controls which are uniquely in one of said groups, and shared controls which are present in more than one of said groups.

105. A system as in claim 6 in which said protected processing environment selects at least one of the alternate groups of controls from said first control set.

106. A system as in claim 8 in which said protected processing environment selects at least one of the alternate groups of controls from said second control set.

107. A method as in claim 9 in which said first secure control set is made up of controls from at least two alternate groups of controls.

108. A method as in claim 107 in which said at least two alternate groups of controls include controls which are uniquely in one of said groups, and shared controls which are present in more than one of said groups.

109. A method as in claim 9 in which said second secure control set is made up of controls from at least two alternate groups of controls.

110. A method as in claim 109 in which said at least two alternate groups of controls making up said second secure control set include controls which are uniquely in one of said groups, and shared controls which are present in more than one of said groups.

111. A method as in claim 107 in which said step of electronically negotiating includes a step of selecting at least one of the alternate groups of controls from said first secure control set.

112. A method as in claim 109 in which said step of electronically negotiating includes a step of selecting at least one of the alternate groups of controls from said second secure control set.

113. A method as in claim 1 in which said first control set, said second control set or said negotiated control set includes a REGISTER control.

114. A method as in claim 1 in which said first control set, said second control set or said negotiated control set includes a WANT control.

115. A method as in claim 1 in which said first control set, said second control set or said negotiated control set includes a REQUIRE control.

116. A system as in claim 2 in which said first secure control set, said second secure control set or said third control set includes an ACCEPT control.

117. A system as in claim 2 in which said first secure control set, said second secure control set or said third control set includes a REJECT control.

118. A system as in claim 2 in which said first secure control set, said second secure control set or said third control set includes an OFFER control.

119. A system as in claim 3 in which said first secure control set, said second secure control set, or said electronic contract includes a HAVE control.

120. A system as in claim 3 in which said first secure control set, said second secure control set, or said electronic contract includes a QUIT control.

121. A system as in claim 1 in which said first secure control set, said second secure control set or said electronic contract includes an AGREEMENT control.

122. A system as in claim 6 in which said first control set or said second set includes a WANT control and a REQUIRE control.

123. A system as in claim 6 in which said first control set or said second set includes a REGISTER control and a WANT control.

124. A system as in claim 6 in which said negotiated control set includes an AGREEMENT control.

125. A method as in claim 9 in which said first secure control set includes a REGISTER control and an OFFER control.

126. A method as in claim 9 in which said second secure control set includes an OFFER control and a HAVE control.

127. A method as in claim 9 in which said electronic contract includes a REGISTER control and an AGREEMENT control.

128. A method as in claim 1 further including the step of executing said negotiated control set within said protected processing environment.

129. A method as in claim 128 further including the step of executing said negotiated control set within a second protected processing environment which is different from the protected processing environment within which said performing step occurs.

130. A system as in claim 2 further including means for executing said third control set within a protected processing environment.

131. A system as in claim 130 in which said protected processing environment is located at said second location.

132. A system as in claim 130 in which said protected processing environment is located at a location other than said second location.

133. A system as in claim 3 further including means for executing said electronic contract within a protected processing environment.

134. A system as in claim 133 in which said protected processing environment is located at said second location.

135. A system as in claim 133 in which said protected processing environment is located at a location other than said second location.

136. A system as in claim 6 in which said negotiated control set is executed in said protected processing environment.

137. A system as in claim 6 in which said negotiated control set is executed in a second protected processing environment.

138. A method as in claim 9 further including the step of executing said electronic contract.

139. A method as in claim 138 in which said step of executing said electronic contract occurs in a protected processing environment.

140. A method as in claim 139 in which said protected processing environment is located at said second location.

141. A method as in claim 138 in which said protected processing environment is located at a location other than said second location.

142. A method as in claim 1 in which said negotiated control set is digitally signed.

143. A method as in claim 1 in which said negotiated control set is digitally signed by said first control set.

144. A method as in claim 143 in which said negotiated control set is digitally signed by said second control set.

145. A method as in claim 1 in which said negotiated control set is digitally signed by a control set which carries out said electronic negotiation.

146. A method as in claim 142 in which said digital signing is done through public key encryption.

147. A system as in claim 142 further including means for digitally signing said third control set.

148. A system as in claim 147 in which said means for digitally signing said third control set includes means for allowing said first

secure control set to carry out said digital signing.

149. A system as in claim 147 in which said means for digitally signing said third control set includes means for allowing said second secure control set to carry out said digital signing.

150. A system as in claim 3 further including means for digitally signing said electronic contract.

151. A system as in claim 150 in which said means for digitally signing said electronic contract includes means for allowing said first secure control set to carry out said digitally signing.

152. A system as in claim 150 in which said means for digitally signing said electronic contract includes means for allowing said second secure control set to carry out said digitally signing.

153. A system as in claim 6 in which said protected processing environment digitally signs said negotiated control set.

154. A system as in claim 153 in which said protected processing environment digitally signs said negotiated control set using a digital signature created or supplied by said first control set.

155. A system as in claim 153 in which said protected processing environment digitally signs said negotiated control set using a digital signature created or supplied by said second control set.

156. A method as in claim 9 further including digitally signing said electronic contract.

157. A method as in claim 156 in which said step of digitally signing said electronic contract is carried out using a digital signature created or supplied at least in part by said first secure control set.

158. A method as in claim 156 in which said step of digitally signing said electronic contract is carried out using a digital signature created or supplied at least in part by said second secure control set.

159. A method as in claim 1 in which said negotiated control set includes controls containing human-language terms corresponding to at least certain of the machine-executable controls contained in said negotiated control set.

160. A method as in claim 159 in which said human-language terms are contained in one or more data descriptor data structures.

161. A system as in claim 2 in which said third control set includes controls containing human-language terms corresponding to at least certain of the machine-executable controls contained in said third control set.

162. A method as in claim 161 in which said human-language terms are contained in one or more data descriptor data structures.

163. A system as in claim 3 in which said electronic contract includes controls containing human-language terms corresponding to at least certain of the machine-executable controls contained in said electronic contract.

164. A method as in claim 163 in which said human-language terms are contained in one or more data descriptor data structures.

165. A system as in claim 6 in which said negotiated control set includes controls containing human-language terms corresponding to at least certain of the machine-executable controls contained in said negotiated control set.

166. A method as in claim 165 in which said human-language terms are contained in one or more data descriptor data structures.

167. A method as in claim 9 in which said electronic contract includes controls containing human-language terms corresponding to at least certain of the machine-executable controls contained in said electronic contract.

168. A method as in claim 167 in which said human-language terms are contained in one or more data descriptor data structures.

169. A method as in claim 1 in which said remote site contains a second protected processing environment.

170. A system as in claim 2 in which said means for creating a first secure control set includes a protected processing environment.

171. A system as in claim 2 in which said means for creating a second secure control set includes a protected processing environment.

172. A system as in claim 2 in which said means at said second location for securely integrating includes a protected processing environment.

173. A system as in claim 3 in which said means for creating a first secure control set includes a protected processing environment.

174. A system as in claim 3 in which said means for creating a second secure control set includes a protected processing environment.

175. A system as in claim 3 in which said negotiation means includes a protected processing environment.

176. A method as in claim 9 in which said first location includes a protected processing environment.

177. A method as in claim 9 in which said second location includes a protected processing environment.

178. A method as in claim 1 in which said first protected processing environment contains a first secure processing unit.

179. A method as in claim 178 in which said steps of performing and producing are carried out, at least in part, by said first secure processing unit.

180. A method as in claim 178 in which said second protected processing environment contains a second secure processing unit.

181. A system as in claim 2 in which said means for creating a first secure control set includes a first secure processing unit.

182. A system as in claim 181 in which said means for creating a second secure control set includes a second secure processing unit.

183. A system as in claim 182 in which said means at said second location for securely integrating includes said second secure processing unit.

184. A system as in claim 3 in which said means for creating a first secure control set includes a secure processing unit.

185. A system as in claim 3 in which said means for creating a second secure control set includes a secure processing unit.

186. A system as in claim 3 in which said negotiating means includes a secure processing unit.

187. A system as in claim 6 in which said protected processing environment includes a secure processing unit.

188. A method as in claim 9 in which said first location contains a secure processing unit.

189. A method as in claim 188 in which said second location contains a second secure processing unit.

190. A method as in claim 189 in which said step of securely executing at least a portion of said first and second secure control sets is performed at least in part using said second secure processing unit.

191. A method as in claim 1 in which said protected processing environment contains a software based tamper resistant barrier.

192. A method as in claim 191 in which said steps of performing and producing are carried out, at least in part, within said software based tamper resistant barrier.

193. A method as in claim 169 in which said first protected processing environment contains a first software based tamper resistant barrier.

194. A method as in claim 193 in which said second protected processing environment contains a second software based tamper resistant barrier.

195. A system as in claim 2 in which said first location contains a first software based tamper resistant barrier.

196. A system as in claim 195 in which said second location contains a second software based tamper resistant barrier.

197. A system as in claim 3 in which said first location contains a first software based tamper resistant barrier.

198. A system as in claim 3 in which said second location contains a second software based tamper resistant barrier.

199. A system as in claim 6 in which said protected processing environment includes a software based tamper resistant barrier.

200. A method as in claim 9 in which said first location contains a

first software based tamper resistant barrier.

201. A method as in claim 200 in which said second location contains a second software based tamper resistant barrier.

202. A method as in claim 1 in which said first control set represents a negotiating position of a first party.

203. A method as in claim 202 in which said first party is a clearinghouse.

204. A method as in claim 202 in which said first party is a content provider.

205. A method as in claim 202 in which said first party is a content distributor.

206. A method as in claim 202 in which said first party is a content user.

207. A method as in claim 202 in which said second control set represents a negotiating position of a second party.

208. A method as in claim 207 in which said second party is a clearinghouse.

209. A method as in claim 207 in which said second party is a content provider.

210. A method as in claim 207 in which said second party is a content distributor.

211. A method as in claim 207 in which said second party is a content user.

212. A system as in claim 2 in which said first secure control set represents a negotiating position of a first party.

213. A system as in claim 212 in which said first party is a clearinghouse.

214. A system as in claim 212 in which said first party is a content provider.

215. A system as in claim 212 in which said first party is a content distributor.

216. A system as in claim 212 in which said first party is a content user.

217. A system as in claim 212 in which said second control set represents a negotiating position of a second party.

218. A method as in claim 217 in which said second party is a clearinghouse.

219. A method as in claim 217 in which said second party is a content provider.

220. A method as in claim 217 in which said second party is a content distributor.

221. A method as in claim 217 in which said second party is a content user.

222. A system as in claim 3 in which said first secure control set represents a negotiating position of a first party.

223. A system as in claim 222 in which said first party is a clearinghouse.

224. A system as in claim 222 in which said first party is a content provider.

225. A system as in claim 222 in which said first party is a content distributor.

226. A system as in claim 222 in which said first party is a content user.

227. A system as in claim 222 in which said second control set represents a negotiating position of a second party.

228. A method as in claim 227 in which said second party is a clearinghouse.

229. A method as in claim 227 in which said second party is a content provider.

230. A method as in claim 227 in which said second party is a content distributor.

231. A method as in claim 227 in which said second party is a content user.

232. A system as in claim 6 in which said first control set represents a negotiating position of a first party.

233. A system as in claim 232 in which said first party is a clearinghouse.

234. A system as in claim 232 in which said first party is a content

provider.

235. A system as in claim 232 in which said first party is a content distributor.

236. A system as in claim 232 in which said first party is a content user.

237. A system as in claim 232 in which said second control set represents a negotiating position of a second party.

238. A method as in claim 237 in which said second party is a clearinghouse.

239. A method as in claim 237 in which said second party is a content provider.

240. A method as in claim 237 in which said second party is a content distributor.

241. A method as in claim 237 in which said second party is a content user.

242. A method as in claim 9 in which said first secure control set represents a negotiating position of a first party.

243. A method as in claim 242 in which said first party is a clearinghouse.

244. A method as in claim 242 in which said first party is a content provider.

245. A method as in claim 242 in which said first party is a content distributor.

246. A method as in claim 242 in which said first party is a content user.

247. A method as in claim 242 in which said second control set represents a negotiating position of a second party.

248. A method as in claim 247 in which said second party is a clearinghouse.

249. A method as in claim 247 in which said second party is a content provider.

250. A method as in claim 247 in which said second party is a content distributor.

251. A method as in claim 247 in which said second party is a content user.

252. A method as in claim 1 in which said first control set contains controls governing the type of payment mechanism to be used for a transaction.

253. A method as in claim 1 in which said first control set contains controls governing the price to be used for a transaction.

254. A method as in claim 1 in which said first control set contains controls governing the auditing method to be used for a transaction.

255. A method as in claim 1 in which said first control set contains controls governing the identity of the clearinghouse to be used for a transaction.

256. A method as in claim 1 in which said first control set contains controls governing the information to be disclosed in a transaction.

257. A method as in claim 1 in which said second control set contains controls governing the type of payment mechanism to be used for a transaction.

258. A method as in claim 1 in which said second control set contains controls governing the price to be used for a transaction.

259. A method as in claim 1 in which said second control set contains controls governing the auditing method to be used for a transaction.

260. A method as in claim 1 in which said second control set contains controls governing the identity of the clearinghouse to be used for a transaction.

261. A method as in claim 1 in which said second control set contains controls governing the information to be disclosed in a transaction.

262. A method as in claim 1 in which said negotiated control set contains controls governing the type of payment mechanism to be used for a transaction.

263. A method as in claim 1 in which said negotiated control set contains controls governing the price to be used for a transaction.

264. A method as in claim 1 in which said negotiated control set contains controls governing the auditing method to be used for a

transaction.

265. A method as in claim 1 in which said negotiated control set contains controls governing the identity of the clearinghouse to be used for a transaction.

266. A method as in claim 1 in which said negotiated control set contains controls governing the information to be disclosed in a transaction.

267. A system as in claim 2 in which said first secure control set contains controls governing the type of payment mechanism to be used for a transaction.

268. A system as in claim 2 in which said first secure control set contains controls governing the price to be used for a transaction.

269. A system as in claim 2 in which said first secure control set contains controls governing the auditing method to be used for a transaction.

270. A system as in claim 2 in which said first secure control set contains controls governing the identity of the clearinghouse to be used for a transaction.

271. A system as in claim 2 in which said first secure control set contains controls governing the information to be disclosed in a transaction.

272. A system as in claim 2 in which said second secure control set contains controls governing the type of payment mechanism to be used for a transaction.

273. A system as in claim 2 in which said second secure control set contains controls governing the price to be used for a transaction.

274. A system as in claim 2 in which said second secure control set contains controls governing the auditing method to be used for a transaction.

275. A system as in claim 2 in which said second secure control set contains controls governing the identity of the clearinghouse to be used for a transaction.

276. A system as in claim 2 in which said second secure control set contains controls governing the information to be disclosed in a transaction.

277. A system as in claim 2 in which said third control set contains controls governing the type of payment mechanism to be used for a transaction.

278. A system as in claim 2 in which said third control set contains controls governing the price to be used for a transaction.

279. A system as in claim 2 in which said third control set contains controls governing the auditing method to be used for a transaction.

280. A system as in claim 2 in which said third control set contains governing the identity of the clearinghouse to be used for a transaction.

281. A system as in claim 2 in which said third control set contains controls governing the information to be disclosed in a transaction.

282. A system as in claim 3 in which said first secure control set contains controls governing the type of payment mechanism to be used for a transaction.

283. A system as in claim 3 in which said first secure control set contains controls governing the price to be used for a transaction.

284. A system as in claim 3 in which said first secure control set contains controls governing the auditing method to be used for a transaction.

285. A system as in claim 3 in which said first secure control set contains controls governing the identity of the clearinghouse to be used for a transaction.

286. A system as in claim 3 in which said first secure control set contains controls governing the information to be disclosed in a transaction.

287. A system as in claim 3 in which said second secure control set contains controls the type of payment mechanism to be used for a transaction.

288. A system as in claim 2 in which said second secure control

set contains controls governing the price to be used for a transaction.

289. A system as in claim 2 in which said second secure control set contains controls governing the auditing method to be used for a transaction.

290. A system as in claim 2 in which said second secure control set contains controls governing the identity of the clearinghouse to be used for a transaction.

291. A system as in claim 2 in which said second secure control set contains controls governing the information to be disclosed in a transaction.

292. A system as in claim 2 in which said electronic contract contains controls governing the type of payment mechanism to be used for a transaction.

293. A system as in claim 2 in which said electronic contract contains controls governing the price to be used for a transaction.

294. A system as in claim 2 in which said electronic contract contains controls governing the auditing method to be used for a transaction.

295. A system as in claim 3 in which said electronic contract contains controls governing the identity of the clearinghouse to be used for a transaction.

296. A system as in claim 3 in which said electronic contract contains controls governing the information to be disclosed in a transaction.

297. A system as in claim 6 in which said first control set contains controls the type of payment mechanism to be used for a transaction.

298. A system as in claim 6 in which said first control set contains controls governing the price to be used for a transaction.

299. A system as in claim 6 in which said first control set contains controls governing the auditing method to be used for a transaction.

300. A system as in claim 6 in which said first control set contains controls governing the identity of the clearinghouse to be used for a transaction.

301. A system as in claim 6 in which said first control set contains controls governing the information to be disclosed in a transaction.

302. A system as in claim 6 in which said second control set contains controls governing the type of payment mechanism to be used for a transaction.

303. A system as in claim 6 in which said second control set contains controls governing the price to be used for a transaction.

304. A system as in claim 6 in which said second control set contains controls governing the auditing method to be used for a transaction.

305. A system as in claim 6 in which said second control set contains controls governing the identity of the clearinghouse to be used for a transaction.

306. A system as in claim 6 in which said second control set contains controls governing the information to be disclosed in a transaction.

307. A system as in claim 6 in which said negotiated control set contains controls governing the type of payment mechanism to be used for a transaction.

308. A system as in claim 6 in which said negotiated control set contains controls governing the price to be used for a transaction.

309. A system as in claim 6 in which said negotiated control set contains controls governing the auditing method to be used for a transaction.

310. A system as in claim 6 in which said negotiated control set contains controls governing the identity of the clearinghouse to be used for a transaction.

311. A system as in claim 6 in which said negotiated control set contains controls governing the information to be disclosed in a transaction.

312. A method as in claim 9 in which said first secure control set contains controls governing the type of payment mechanism to be used for a transaction.

313. A method as in claim 9 in which said first secure control set contains controls governing the price to be used for a transaction.

314. A method as in claim 9 in which said first secure control set contains controls governing the auditing method to be used for a transaction.

315. A method as in claim 9 in which said first secure control set governing the identity of the clearinghouse to be used for a transaction.

316. A method as in claim 9 in which said first secure control set contains controls governing the information to be disclosed in a transaction.

317. A method as in claim 9 in which said second secure control set contains controls governing the type of payment mechanism to be used for a transaction.

318. A method as in claim 9 in which said second secure control set contains controls governing the price to be used for a transaction.

319. A method as in claim 9 in which said second secure control set contains controls governing the auditing method to be used for a transaction.

320. A method as in claim 9 in which said second secure control set governing the identity of the clearinghouse to be used for a transaction.

321. A method as in claim 9 in which said second secure control set contains controls governing the information to be disclosed in a transaction.

322. A method as in claim 9 in which said negotiated control set contains controls governing the type of payment mechanism to be used for a transaction.

323. A method as in claim 9 in which said negotiated control set contains controls governing the price to be used for a transaction.

324. A method as in claim 9 in which said negotiated control set contains controls governing the auditing method to be used for a transaction.

325. A method as in claim 9 in which said negotiated control set governing the identity of the clearinghouse to be used for a transaction.

326. A method as in claim 9 in which said negotiated control set contains controls governing the information to be disclosed in a transaction.

327. A method as in claim 1 in which said protected processing environment is located at a first site, and said first site includes an operating system based on or compatible with Microsoft Windows.

328. A method as in claim 327 in which said step of performing and producing are carried out, at least in part, by software contained within said operating system.

329. A system as in claim 2 in which said means for creating a first secure control set includes an operating system based on or compatible with Microsoft Windows.

330. A system as in claim 2 in which said means for creating a second secure control set includes an operating system based on or compatible with Microsoft Windows.

331. A system as in claim 2 in which said means at said second location for securely integrating said first and second control sets includes an operating system based on or compatible with Microsoft Windows.

332. A system as in claim 3 in which said means for creating a first secure control set includes an operating system based on or compatible with Microsoft Windows.

333. A system as in claim 3 in which said means for creating a second secure control set includes an operating system based on or compatible with Microsoft Windows.

334. A system as in claim 3 in which said negotiation means includes an operating system based on or compatible with Microsoft Windows.

335. A system as in claim 6 in which said protected processing environment includes an operating system based on or compatible with Microsoft Windows.

336. A method as in claim 9 in which said first location includes a first operating system based on or compatible with Microsoft Windows.

337. A method as in claim 336 in which said second location includes a second operating system based on or compatible with Microsoft Windows.

338. A method as in claim 336 in which said step of creating a first secure control is carried out at least in part by software incorporated in said first operating system.

339. A method as in claim 337 in which said step of creating a second secure control is carried out at least in part by software incorporated in said second operating system.

340. A method as in claim 337 in which said step of electronically negotiating is carried out at least in part by software incorporated in said second operating system.

341. A method as in claim 1 further comprising said negotiated control set governing the use of digital information.

342. A method as in claim 1 further comprising said negotiated control set governing the execution of at least one load module.

343. A method as in claim 1 further comprising said negotiated control set governing the execution of at least one method.

344. A method as in claim 1 further comprising said negotiated control set governing the execution of at least one other control set different from said first control set, said second control set and said negotiated control set.

345. A system as in claim 2 further comprising means by which said third control set governs the use of digital information.

346. A system as in claim 2 further comprising means by which said third control set governs the execution of at least one load module.

347. A system as in claim 2 farther comprising means by which said third control set governs the execution of at least one method.

348. A system as in claim 2 further comprising means by which said third control set governs the execution of at least one transaction.

349. A system as in claim 2 further comprising means by which said third control set governs the execution of at least one procedure.

350. A system as in claim 2 further comprising means by which said third control set governs the execution of at least one other control set different from said first control set, said second control set and said third control set.

351. A system as in claim 3 further comprising means by which said electronic contract governs the use of digital information.

352. A system as in claim 3 further comprising means by which said electronic contract governs the execution of at least one load module.

353. A system as in claim 3 further comprising means by which said electronic contract governs the execution of at least one method.

354. A system as in claim 3 further comprising means by which said electronic contract governs the execution of at least one transaction.

355. A system as in claim 3 further comprising means by which said electronic contract governs the execution of at least one procedure.

356. A system as in claim 3 further comprising means by which said electronic contract governs the execution of a third control set different from said first control set and said second control set.

357. A system as in claim 6 further comprising means by which said negotiated control set governs the use of digital information.

358. A system as in claim 6 further comprising means by which said negotiated control set governs the execution of at least one load module.

359. A system as in claim 6 further comprising means by which said negotiated control set governs the execution of at least one method.

360. A system as in claim 6 further comprising means by which

said negotiated control set governs the execution of at least one transaction.

361. A system as in claim 6 further comprising means by which said negotiated control set governs the execution of at least one procedure.

362. A system as in claim 6 further comprising means by which said negotiated control set governs the execution of a third control set different from said first control set and said second control set.

363. A method as in claim 9 further comprising said electronic contract governing the use of digital information.

364. A method as in claim 9 further comprising said electronic contract governing the execution of at least one load module.

365. A method as in claim 9 further comprising said electronic contract governing the execution of at least one method.

366. A method as in claim 9 further comprising said electronic contract governing the execution of at least one transaction.

367. A method as in claim 9 further comprising said electronic contract governing the execution of at least one procedure.

368. A method as in claim 9 further comprising said electronic contract governing the execution of at least one other control set different from said first control set, said second control set and said negotiated control set.

369. A method for securely managing electronic negotiations related to electronic commerce value chain activities including:

- employing a first protected processing environment to securely specify rules and/or controls for managing an electronic commerce process;
- securely making said specified rules and/or controls available to a second protected processing environment, located remotely from said first protected processing environment;
- employing said second protected processing environment to further securely specify rules and/or controls for managing at least one commerce process related to the common commercial interests of at least two parties;
- employing said second protected processing environment to securely electronically negotiate at least one aggregate rules and/or controls set representing the electronic interests of said at least two parties; and
- employing a protected processing environment to manage said electronic commerce process consistent with at least a portion of said aggregate rules and/or controls set.

370. A system for securely managing electronic negotiations related to electronic commerce value chain activities including:

- a first protected processing environment associated with a first party, for securely specifying rules and/or controls for managing an electronic commerce process, and for securely making said specified rules and/or controls available to a second party;
- a second protected processing environment associated with a second party different from said first party, for
- further securely specifying rules and/or controls, including means for managing at least one commerce process related to the common commercial interests of said first party and said second party;
- securely electronically negotiating at least one aggregate rules and/or controls set representing the electronic interests of both said first party and said second party; and
- managing said electronic commerce process consistent with said at least a portion of said aggregate rules and/or controls set.

371. A system for negotiating electronic contracts, comprising:

- a storage arrangement that stores a first control set received from a remote site, and stores a second control set;
- a protected processing environment, coupled to said storage arrangement, that:
- performs an electronic negotiation between said first control set and said second control set,
- provides interaction between said first and second control sets, and
- produces negotiated control information resulting from said interaction between said first and second control sets.

372. A system as in claim 371 further including means for electronically enforcing said negotiated control set.
373. A system as in claim 371 further including means for generating an electronic contract based on said negotiated control set.
374. A system as in claim 3 in which said electronic contract is contained, at least in part, in a User Rights Table.
375. A method as in claim 9 in which said electronic contract is contained, at least in part, in a User Rights Table.
■

This is a divisional of application Ser. No. 08/388,107, filed Feb. 13, 1995, abandoned.
■

Background/Summary: Show background/summary
■
Drawing Descriptions: Show drawing descriptions
■
Description of Preferred Embodiments: Show description of preferred embodiments
■
Foreign References:

Publication	Country	Date	IPC Class
EP1984000128672	European Patent Office (EPO)	12 /1984	
EP1986000180460	European Patent Office (EPO)	5 /1986	
EP1988000370146	European Patent Office (EPO)	11 /1988	
EP19900399822A2	European Patent Office (EPO)	11 /1990	
EP19910421409A2	European Patent Office (EPO)	4 /1991	
EP19910456386A2	European Patent Office (EPO)	11 /1991	
EP19920469864A3	European Patent Office (EPO)	2 /1992	
EP19920469864A2	European Patent Office (EPO)	2 /1992	
EP19930565314A2	European Patent Office (EPO)	10 /1993	
EP19940593305A2	European Patent Office (EPO)	4 /1994	
EP19950651554A1	European Patent Office (EPO)	5 /1995	
EP19950668695A2	European Patent Office (EPO)	8 /1995	
EP19960696798A1	European Patent Office (EPO)	2 /1996	
EP19960695985A1	European Patent Office (EPO)	2 /1996	
EP1996000725376	European Patent Office (EPO)	8 /1996	
EP19960749081A1	European Patent Office (EPO)	12 /1996	
EP19970778513A2	European Patent Office (EPO)	6 /1997	

EP19970795873A2	European Patent Office (EPO)	9 /1997	
DE1990038039821	Germany	1 /1990	
JP1987000241061	Japan	10 /1987	
JP1989000068835	Japan	3 /1989	
JP1989000068835	Japan	3 /1989	
JP1990000242352	Japan	9 /1990	
JP1990000247763	Japan	10 /1990	
JP1990000294855	Japan	12 /1990	
JP1992000369068	Japan	12 /1992	
JP1993000181734	Japan	7 /1993	
JP1993000257783	Japan	10 /1993	
JP1993000268415	Japan	10 /1993	
JP1994000001757	Japan	6 /1994	
JP1994000215010	Japan	8 /1994	
JP1994006225059	Japan	8 /1994	
JP1995000056794	Japan	3 /1995	
JP1995000084852	Japan	3 /1995	
JP1995000141138	Japan	6 /1995	
JP1995000200317	Japan	8 /1995	
JP1995000200492	Japan	8 /1995	
JP1995000244639	Japan	9 /1995	
JP1996000137795	Japan	5 /1996	
JP1996000152990	Japan	6 /1996	
JP1996000185298	Japan	7 /1996	
GB1993002264796	United Kingdom	9 /1993	
GB1996002294348	United Kingdom	4 /1996	
GB1996002295947	United Kingdom	6 /1996	
WO1990WO0002382	World Intellectual Property Organization (WIPO)	3 /1990	
WO1992WO0006438	World Intellectual Property Organization (WIPO)	4 /1992	
WO1992WO0022870	World Intellectual Property Organization (WIPO)	12 /1992	
WO1993WO0001550	World Intellectual Property Organization (WIPO)	1 /1993	
WO1994WO0001821	World Intellectual Property Organization (WIPO)	1 /1994	
WO1994WO0003859	World Intellectual Property Organization (WIPO)	2 /1994	
WO1994WO0006103	World Intellectual Property Organization (WIPO)	3 /1994	
WO1994WO0016395	World Intellectual Property Organization (WIPO)	7 /1994	
WO1994WO0018620	World Intellectual Property Organization (WIPO)	8 /1994	
WO1994WO0022266	World Intellectual Property Organization	9 /1994	

WO1994WO0022266	(WIPO)	9 /1994	
WO1994WO0027406	World Intellectual Property Organization (WIPO)	11 /1994	
WO1995WO0014289	World Intellectual Property Organization (WIPO)	6 /1995	
WO1996WO0000963	World Intellectual Property Organization (WIPO)	1 /1996	
WO1996WO0003835	World Intellectual Property Organization (WIPO)	2 /1996	
WO1996WO0005698	World Intellectual Property Organization (WIPO)	2 /1996	
WO1996WO0006503	World Intellectual Property Organization (WIPO)	2 /1996	
WO1996WO0013013	World Intellectual Property Organization (WIPO)	5 /1996	
WO1996WO0021192	World Intellectual Property Organization (WIPO)	7 /1996	
WO1997WO0003423	World Intellectual Property Organization (WIPO)	1 /1997	
WO1997WO0007656	World Intellectual Property Organization (WIPO)	3 /1997	
WO1997WO0032251	World Intellectual Property Organization (WIPO)	9 /1997	
WO1997WO0048203	World Intellectual Property Organization (WIPO)	12 /1997	

Other References:
Article info links by

I S I
————————✦————————
THOMSON SCIENTIFIC

:

- IBM Technical Disclosure Bulletin, "Multimedia Mixed Object Envelopes Supporting a Graduated Fee Scheme via Encryption," vol. 37, No. 03, Mar. 1994, Armonk, NY.
- IBM Technical Disclosure Bulletin, "Transformer Rules for Software Distribution Mechanism-Support Products," vol. 37, No. 04B, Apr. 1994, Armonk, NY.
- Suida, Karl, Mapping New Applications onto New Technologies, "Security Services in Telecommunications Networks," Mar. 8-10, 1988, Zurich.
- Applications Requirements for Innovative Video Programming; How to Foster (or Cripple) Program Development Opportunities for Interactive Video Programs Delivered on Optical Media; A Challenge for the Introduction of DVD (Digital Video Disc) (Oct. 19-20, 1995, Sheraton Universal Hotel, Universal City CA).
- Argent Information Q&A Sheet, http://www.digital-watermark.com/, Copyright 1995, The Dice Company, 7 pages.
- Arneke, David, et al., News Release, AT&T, Jan. 9, 1995, AT&T encryption system protects information services, 1 page.
- AT&T Technology, vol. 9, No. 4, New Products, Systems and Services, pp. 16-19.
- Barassi, Theodore Sedgwick, Esq., The Cybernotary: Public Key Registration and Certificaiton and Authentication of International Legal Transactions, 4 pages.
- Bruner, Rick E., PowerAgent, NetBot help advertisers reach Internet shoppers, Aug. 1997 (Document from Internet).
- CD ROM, Introducing . . . The Workflow CD-ROM Sampler, Creative Networks, MCIMail: Creative Networks, Inc., Palo Alto, California.
- Clark, Tim, Ad service gives cash back, www.news.com, Aug. 4, 1997, 2 pages (Document from Internet).
- Communications of the ACM, Jun. 1996, vol. 39, No. 6.
- Cunningham, Donna, et al., News Release, AT&T, Jan. 31, 1995, AT&T, VLSI Technology join to improve info highway security, 3 pages.
- Data Sheet, About the Digital Notary Service, Surety Technologies, Inc., 1994-95, 6 pages.
- Dempsey, et al., D-Lib Magazine, Jul./Aug. 1996 The Warwick Metadata

Workshop: A Framework for the Deployent of Resource Description, Jul. 15, 1966.
- DiscStore (Electronic Publishing Resources 1991).
- Document from Internet, cgi@ncsa.uiuc.edu, CGI Common Gateway Interface, 1 page, 1996.
- DSP56000/DSP56001 Digital Signal Processor User's Manual, Motorola, 1990, p. 2-2.
- Dusse, Stephen R. and Burton S. Kaliski A Cryptographic Library for the Motorola 56000 in Damgard, I. M., Advances in Cryptology--Proceedings Eurocrypt 90, Springer-Verlag, 1991, pp. 230-244. (15 pages) 16 patents reference this [Article info]
- Dyson, Esther, Intellectual Value, Wired Magazine, Jul. 1995, pp. 136-141 and 182-184.
- Electronic Publishing Resources Inc. Protecting Electronically Published Properties Increasing Publishing Profits (Electronic Publishing Resources 1991).
- Firefly Network, Inc., www.ffly.com, What is Firefly? Firefly revision: 41.4 Copyright 1995, 1996.
- Gleick, James, "Dead as a Dollar" The New York Times Magazine, Jun. 16, 1996, Section 6, pp. 26-30, 35, 42, 50, 54.
- Greguras, Fred, Softic Symposium '95, Copyright Clearances and Moral Rights, Nov. 30, 1995 (as updated Dec. 11, 1995), 3 pages.
- Guillou, L.: Smart Cards and Conditional Access, pp. 480-490 Advances in Cryptography, Proceedings of EuroCrypt 84 (Beth et al, Ed., Springer-Verlag 1985).
- Harman, Harry H., Modern Factor Analysis, Third Edition Revised, University of Chicago Press Chicago and London, Third revision published 1976.
- Herzberg, Amir et al., Public Protection of Software, ACM Transactions on Computer Systems, vol. 5, No. 4, Nov. 1987, pp. 371-393. (23 pages)
- Holt, Stannie, Start-up promises user confidentiality in Web marketing service, Info World Electric, Aug. 13, 1997 (Document from Internet).
- Hotjava.TM.: The Security Story, 4 pages.
- Invoice? What is an Invoice? Business Week, Jun. 10, 1996.
- Javasoft, Frequently Asked Questions--Applet Security, What's Java.TM.? Products and Services, Java/Soft News, Developer's Cornier,Jun. 7, 1996, 8 pages.
- Jiang, et al, A concept-Based Approach to Retrieval from an Electronic Industrialn Directory, International Journal of Electronic Commerce, vol. 1, No. 1, Fall 1996, pp. 51-72.
- Jones, Debra, Top Tech Stories, PowerAgent Introducts First Internet `Infomediary` to Empower and Protect Consumers, Aug. 13, 1997 3 pages (Document from Internet).
- Kohntopp, M., Sag's durch bie Blume, Apr. 1996, marit@schulung.netuse.de.
- Lagoze, Carl, D-Lib Magazine, Jul./Aug. 1996, The Warwick Framework, A Container Architecture for Diverse Sets of Metadata.
- Maclachlan, Malcolm, PowerAgent Debuts Spam-Free Marketing, TechWire, Aug. 13, 1997, 3 pages (Document from Internet).
- Milbrandt, E., Stenanography Info and Archive, 1996.
- Mori, Ryoichi and Masaji Kawahara, The Transactions of the EIEICE, V, Superdistribution: The Concept and the Architecture, E73 (Jul. 1990), No. 7, Tokyo, Japan.
- Mossberg, Walter S., Personal Technology, Threats to Privacy On-Line Become More Worrisome, Wall Street Journal, Oct. 24, 1996.
- Negroponte, Electronic Word of Mouth, Wired Oct. 1996, p. 218.
- News Release, Premenos Announces Templar 2.0--Next Generation Software for Secure Internet EDI, webmaster@templar.net, 1 page, Jan. 17, 1996.
- News Release, The Document Company Xerox, Xerox Announces Software Kit for Creating Working Documents with Dataglyphs, Nov. 6, 1995, Minneapolis, MN, 13 pages.
- PowerAgent Inc., Proper Use of Consumer Information of the Internet White Paper, Jun. 1997, Document from Internet, 9 pages (Document from

Internet).
- PowerAgent Press Releases, What the Experts are Reporting on PowerAgent, Aug. 13, 1997, 6 pages (Document from Internet).
- PowerAgent Press Releases, What the Experts are Reporting on PowerAgent, Aug. 4, 1997, 5 pages (Document from Internet).
- PowerAgent Press Releases, What the Experts are Reporting on PowerAgent, Aug. 13, 1997, 3 pages (Document from Internet).
- Premenos Corp. White Paper: The Future of Electronic Commerce, A Supplement to Midrange Systems, Internet webmaster@premenos.com, 4 pages.
- Press Release, National Semiconductor and EPR Partner For Information Metering/Data Security Cards (Mar. 4, 1994).
- Rankine G., Thomas--A Complete Single-Chip RSA Device, Advances in Cryptography, Proceedings of Crypto 86, pp. 480-487 (A.M. Odlyzko Ed., Springer-Verlag 1987). (8 pages)
- Resnick, et al., Recommender Systems, Communications of the ACM, vol. 40, No. 3, Mar. 1997, pp. 56-89. (3 pages) 13 patents reference this [Article info]
- ROI (Personal Library Software, 1987 or 1988).
- ROI-Solving Critical Electronic Publishing Problems (Personal Library Software, 1987 or 1988).
- Rothstein, Edward, The New York Times, Technology, Connections, Making th eInternet come to you, through `push` technology . . . p. D5, Jan. 20, 1997.
- Rutkowski, Ken, PowerAgent Introduces First Internet `Infomediary` to Empower and Protect Consumers, Tech Talk News Story, Aug. 4, 1997 (Document from Internet).
- Sager, Ira (Edited by), Bits & Bytes, Business Week, Sep. 23, 1996, p. 142E.
- Schurmann, Jurgen, Pattern Classification, A Unified View of Statistical and Neural Approaches, John Wiley & Sons, Inc., 1996.
- Shear, Solutions for CD-ROM Pricing and Data Security Problems, pp. 530-533, CD ROM Yearbook 1988-1989 (Microsoft Press 1988 or 1989).
- Special Report, The Internet:Fulfilling the Promise The Internet: Bring Order From Chaos; Lynch, Clifford, Search the Internet; Resnick, Paul, Filtering Information on the Internet; Hearst, Marti A., Interfaces for Searching the Web; Stefik, Mark, Trusted Systems; Scientific American, Mar. 1997, pp. 49-56, 62-64, 68-72, 78-81.
- Stefik, Internet Dreams: Archetypes, Myths, and Metaphors, Letting Loose the Light: Igniting Commerce in Electronic Publication, pp. 219-253, (1996) Massachusetts Institute of Technology.
- Stefik, Mark, Introduction to Knowledge Systems, Chapter 7, Classification, pp. 543-607, 1995 by Morgan Kaufmann Publishers, Inc.
- Stefik, Mark, Letting Loose the Light, Igniting Commerce in Electronic Publication, (1994, 1995) Palo Alto, California.
- Struif, Bruno The Use of Chipcards for Electronic Signatures and Encryption in: Proceedings for the 1989 Conference on VSLI and Computer Peripherals, IEEE Computer Society Press, 1989, pp. 4/155-4/158.
- Templar Overview,: Premenos, Internet info@templar.net, 4 pages.
- Templar Software and Services: Secure, Reliable, Standards-Based EDI Over the Internet, Prementos, Internet info@templar.net, 1page.
- The Benefits of ROI For Database Protection and Usage Based Billing (Personal Library Software, 1987 or 1988).
- Voight, Joan, Beyond the Banner, Wired, Dec. 1996, pp. 196, 200, 204.
- Vonder Haar, Steven, PowerAgent Launches Commercial Service, Inter@ctive Week, Aug. 4, 1997 (Document from Internet).
- Weber, Dr. Robert, Digital Rights Management Technologies, A Report to the International Federation of Reproduction Rights Organisations, Oct. 1995,pp. 1-49.
- Weber, Dr. Robert, Digital Rights Management Technologies, Oct. 1995, 21 pages.
- Weber, Metering Technologies for Digital Intellectual Property, A Report to the International Federation of Reproduction Rights Organisations, pp. 1-29; Oct. 1994, Boston, MA, USA.

- Wepin Store, Stenography (Hidden Writing) (Common Law 1995).
- World Wide Web FAQ, How can I put an access counter on my home page?, 1 page, 1996.
- Yellin, F. Low Level Security in Java, 8 pages.
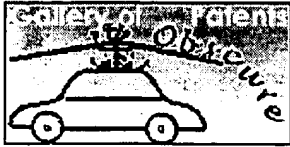
Nominate this invention for the Gallery...

Alternative Searches

Patent Number

Boolean Text

Advanced Text

Browse

U.S. Class by title

U.S. Class by number

IP Listing Search

IBM Technical Disclosure Bulletin

Derwent World Patents Index

disclosures@IP.Com